UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/686,343	10/14/2003	Ernie Brickell	042390.P15784	7197

45209 7590 06/17/2008

INTEL/BLAKELY
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
06/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/686,343	BRICKELL ET AL.	
	Examiner	Art Unit	
	Leynna T. Truvan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 April 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-10,12-18 and 20* is/are pending in the application.

4a) Of the above claim(s) *3,11 and 19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-10,12-18 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-2, 4-10, 12-18, and 20 are pending.

Claims 3, 11, and 19 remains cancelled.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/7/08 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1-2, 4-10, 12-18, and 20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 9, and 17 recites wherein the delegated environment is an environment to which the master owner token is not communicated. This is new subject matter that was not originally filed nor

supported by the specification. Specification discusses the delegate owner token being communicated and partial functionality that is unable to modify master owner token. Whereas, the master owner token have full owner functionality that have the ability to modify the MOT and the ME may generate the MOT when the ME is first executed by the computer system [0021 + 0023]. However, specification does not limit the claimed the delegated environment is an environment to which the master owner token is not communicated.

All dependent claims are also rejected by virtue of their pendency.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 4-10, 12-18, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable by Lambert, et al. (US 7,134,138), and further in view of Challener, et al. (US 7,194,762).

As per claim 1:

Lambert discloses a method of managing authorization tokens within a computer system comprising:

creating a master owner token indicating a management environment has full ownership *[of a trusted platform module]* within the computer system; (col.7, lines 55-57)

creating a delegate owner token for a delegated environment (col.8, lines 10-26 and 40-67 and col.22, lines 40- 45), wherein the delegated environment is an environment to which the master owner token is not communicated; (col.4, lines 6-17 and col.14, line 46 – col.15, line 20)

communicating the delegate owner token, to the delegated environment; and (col.9, lines 5-15 and col.22, lines 46-50)

allowing the delegated environment access *[to the trusted platform module]* when the delegated environment presents the delegate owner token to the *[trusted platform module]*. (col.3, line 66 - col.4, line 5 and col.11, lines 5-35)

Lambert discloses the claimed master owner token as the parent or normal access token that have the ownership or privileges that a restricted token does not. The claimed delegate owner token is given as a restricted token that have restricted access or privileges removed relative to its parent token (col.4, lines 5-15 and col.7, lines 54-57). Lambert explains the restricted token is derived from a parent token comprises a reduced subset of access rights/privileges relative to its parent token by altering (lessening) the access rights (col.8, lines 40-67). Lambert discloses the restricted access token have restrictions which have certain rights or privileges to determine whether software can run and the executing environment in which it will run (col.3, line 66 - col.4, line 18). This shows the restricted token is associated with each process which is the claimed environment and enables restricting actions by possibly executable software content (col.9, lines 5-15 and col.11, lines 5-35). Thus, Lambert does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software. Hence, Lambert reads on the claimed creating a delegate owner token for a delegated environment wherein the delegated

environment is an environment to which the master owner token is not communicated. However, Lambert did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19).

As per claim 2: See Lambert on col.7, lines 26-55; discloses the method of claim 1, further comprising storing the master owner token in a secure storage within the computer system.

As per claim 3: Cancelled

As per claim 4: See Lambert on col.8, lines 10-26 and 40-67 and col.22, lines 40- 45; discloses the method of claim 1, wherein creating the delegate owner token comprises the management environment sealing the delegate owner token to the delegated environment.

As per claim 5: See Lambert on col.4, lines 5-15 and col.8, lines 40-67; discloses the method of claim 1, further comprising wherein the master owner token indicating the management environment can change at least one of the master owner token and a delegate owner token.

As per claim 6: See Lambert on col.9, lines 5-15 and col.11, lines 5-35; discloses the method of claim 1, further comprising launching the management environment and then launching the delegated environment.

As per claim 7: See Lambert on col.9, lines 36-67; discloses the method of claim 1, further comprising storing the delegate owner token in an access control list in the resource.

As per claim 8: See Lambert on col.9, lines 36-67 and col.10, lines 20-33; discloses the method of claim 7, further comprising removing, by the management environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

As per claim 9:

Lambert discloses an article comprising:

a storage medium having a plurality of machine readable instructions, wherein when the instructions are executed by a processor, the instructions provide for managing authorization tokens within a computer system by creating a master owner token indicating an administrative environment

has full ownership *[of a trusted platform module]* within the computer system; (col.6, lines 1-37 and col.7, lines 55-57)

creating a delegate owner token for a delegate environment (col.8, lines 10-26 and 40-67 and col.22, lines 40- 45), wherein the delegated environment is an environment to which the master owner token is not communicated; (col.4, lines 6-17 and col.14, line 46 – col.15, line 20)

communicating the delegate owner token to the delegated environment; and (col.9, lines 5-15 and col.22, lines 46-50)

allowing the delegated environment access *[to the trusted platform module]* when the delegated environment presents the delegate owner token *[to the trusted platform module].* (col.3, line 66 - col.4, line 5 and col.11, lines 5-35)

Lambert discloses the claimed master owner token as the parent or normal access token that have the ownership or privileges that a restricted token does not. The claimed delegate owner token is given as a restricted token that have restricted access or privileges removed relative to its parent token (col.4, lines 5-15 and col.7, lines 54-57). Lambert explains the restricted token is derived from a parent token comprises a reduced subset of access rights/privileges relative to its parent token by altering (lessening) the access rights (col.8, lines 40-67). Lambert discloses the restricted access token have restrictions which have certain rights or privileges to determine whether software can run and the executing environment in which it will run (col.3, line 66 - col.4, line 18). This shows the restricted token is associated with each process which is the claimed environment and enables restricting actions by possibly executable software content (col.9, lines 5-15 and col.11, lines 5-35). Thus, Lambert does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software. Hence, Lambert reads

on the claimed creating a delegate owner token for a delegated environment wherein the delegated environment is an environment to which the master owner token is not communicated. However, Lambert did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19).

As per claim 10: See Lambert on col.7, lines 26-55; discloses the article of claim 9, further comprising instructions for storing the master owner token in a secure storage within the computer system.

As per claim 11: Cancelled

As per claim 12: See Lambert on col.8, lines 10-26 and 40-67 and col.22, lines 40- 45; discloses the article of claim 9, wherein creating the delegate owner token comprises the administrative environment sealing the delegate owner token to the delegated environment.

As per claim 13: See Lambert on col.4, lines 5-15 and col.8, lines 40-67; discloses the article of claim 9, further comprising the master owner token indicating the administrative environment can change at least one of the master owner token and the delegate owner token.

As per claim 14: See Lambert on col.9, lines 5-15 and col.11, lines 5-35; discloses the article of claim 9, further comprising instructions for launching the administrative environment and then launching the delegated environment.

As per claim 15: See Lambert on col.9, lines 36-67; discloses the article of claim 9, further comprising instructions for storing the delegate owner token in an access control list in the resource.

As per claim 16: See Lambert on col.9, lines 36-67 and col.10, lines 20-33; discloses the article of claim 9, further comprising instructions for removing, by the administrative environment, the delegate owner token from the access control list and adding a different delegate owner token to the access control list.

As per claim 17:

Lambert discloses a computer system comprising:

a plurality of delegated environments; (col.4, lines 1-4 and col.15, line 61 - col.16, line 24)

a management environment to create a master owner token indicating the management environment has full ownership *[of a trusted platform module]* within the computer system (col.7, lines 55-57), to create a plurality of delegate owner tokens indicating partial ownership (col.8, lines 10-26 and 40-67 and col.22, lines 40- 45) *[of the trusted platform module]*, and to communicate a selected one of the plurality of delegate owner tokens to a selected one of the plurality of delegated environments (col.9, lines 5-15 and col.22, lines 46-50), wherein the selected one of the plurality of delegated environment is an environment to which the master owner token is not communicated; (col.4, lines 6-17 and col.14, line 46 – col.15, line 20)

wherein *[the trusted platform module]* stores delegate owner tokens created by the management environment and allows the selected one of the plurality of delegated environments access *[to the trusted platform module]* when the selected one of the plurality of delegate owner tokens is presented *[to the trusted platform module]* by the selected one of the plurality of delegated environments. (col.3, line 66 - col.4, line 5 and col.11, lines 5-35)

Lambert discloses the claimed master owner token as the parent or normal access token that have the ownership or privileges that a restricted token does not. The claimed delegate owner token is given as a restricted token that have restricted access or privileges removed relative to its parent token (col.4, lines 5-15 and col.7, lines 54-57). Lambert explains the restricted token is derived from a parent token comprises a reduced subset of access rights/privileges relative to its parent token by altering (lessening) the access rights (col.8, lines 40-67). Lambert discloses the restricted access token have restrictions which have certain rights or privileges to determine whether software can run and the executing environment in which it will run (col.3, line 66 - col.4, line 18). This shows the

restricted token is associated with each process which is the claimed environment and enables restricting actions by possibly executable software content (col.9, lines 5-15 and col.11, lines 5-35). Thus, Lambert does not suggest the parent token is communicated to the delegated environment since the focus is the restricted token that is associated to a process/software. Hence, Lambert reads on the claimed creating a delegate owner token for a delegated environment wherein the delegated environment is an environment to which the master owner token is not communicated. However, Lambert did not include a TPM.

Challener discloses a method and system for improved security password-based access to computer networks. The system comprises a server where the server comprises a security chip (col.2, lines 45-49). The invention comprises a security chip, such as a Trusted Platform Module (TPM) where a phrase is signed by the security chip using an encryption key assigned either to the remote user or the security chip (col.2, lines 16-18 and 28-32). The security chip comprises encryption keys, such as a public key/private key pair assigned to the chip (col.2, lines 51-53). Challener discloses a remote user request access to the computer network by providing an ID and password to the server (col.3, lines 4-7). The password is according to the remote user and for access to the server. Challener discloses the system comprising a server (delegated environment) and the remote user password (delegate owner token) where the user's password is given to the server and to the security chip (TPM), rather than the master token being given to the server (col.4, lines 57-59). Further, Challener teaches using a security chip further decreases the exposure to brute force attacks and such TPM allow only certain number of unsuccessful entries of a password before a user is locked (col.3, lines 24-26). So the user of the security chip enforces protection against hardware hammering (col.4, lines 15-19).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Lambert with Challener to teach of a trusted platform module (TPM) because using a security chip decrease the exposure to brute force attacks and enforces protection against hardware hammering (Challener - col.3, lines 24-26 and col.4, lines 18-19).

As per claim 18: See Lambert on col.7, lines 26-55; discloses a computer system of claim 17, further comprising a secure storage to store the master owner token.

As per claim 19: Cancelled

As per claim 20: See Lambert on col.9, lines 36-67 and col.10, lines 20-33; discloses the computer system of claim 19, wherein the trusted platform module comprises an access control list for storing the delegate owner tokens received from the management environment.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135